AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR WARRANTS TO SEARCH AND SEIZE

I, Andrew P. LaRose, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search: the entire premises known as 6 Whittier Road, Merrimack, New Hampshire (NH) 03054 ("TARGET RESIDENCE"), as well as the person of Bryan Scott Hoy ("HOY"). The description of property to be searched is described in the following paragraphs and in Attachment A.

2. This affidavit is made in support of an application seeking authorization to search and seize from the TARGET RESIDENCE, and HOY, all evidence or information as described in Attachment B, which constitutes evidence, fruits, and instrumentalities of violations of Title 18 United States Code (U.S.C.) § 2252(a)(2), which makes it a crime to receive and distribute material depicting the sexual exploitation of a minor; violations of Title 18 U.S.C. § 2252A(a)(5)(A)(B) & (b)(2), which makes it a crime to possess material depicting the sexual exploitation of a minor and access with intent to view it; and violations of Title 18 U.S.C. § 2422(b), which makes it a crime to knowingly persuade or induce a minor to engage in any illegal sexual activity, including attempts.

3. I am a Special Agent of the Federal Bureau of Investigation ("FBI") and have been since December 2022. I received multiple months of law enforcement training at the FBI Academy in Quantico, Virginia. During my training at the FBI Academy, I received specialized training in the methodology of general law enforcement. As such, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

4. I am currently assigned to a Criminal Investigative Squad at the FBI Knoxville

Division, Johnson City Residence Agency. In my current assignment, I am responsible for investigating and identifying various offenses related to crimes against children, and specifically child sexual abuse material ("CSAM"), among other federal violations such as public corruption, civil rights, organized and white-collar crime, and terrorism. I am familiar with law enforcement-related tasks such as executing state and federal search and arrest warrants, processing evidence, and surveilling subjects. I am also familiar with investigations and enforcement of federal child sexual abuse laws in which electronic devices are used as the means for producing, transmitting, collecting, and storing CSAM, as well as information related to other criminal activity.

5. The facts in this affidavit come from my personal observations, training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

6. Based on my training and experience, and on the facts as set forth in this affidavit, I submit there is probable cause that violations of Title 18 U.S.C. § 2252(a)(2), Title 18 U.S.C. § 2252A(a)(5)(A)(B) & (b)(2), and Title 18 U.S.C. § 2422(b), related to the receipt and possession of CSAM, and enticement of a minor to engage in illegal sexual conduct, as further described herein, have been committed by an individual named Bryan Scott Hoy. I further submit there is probable cause to search the location and person described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes, as further described in Attachment B.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

a) "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. See Title 18 U.S.C. § 2256(5).

b) "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

c) "Child Erotica" as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

d) "Child Sexual Abuse Material," as used herein, includes the definition in 18 U.S.C § 2256(8) – any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct – as well as any visual depiction, the production of which involves the use of a minor engaged in "sexually explicit conduct," as that term is defined in 18 U.S.C. § 2256(2).

e) "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

f) "Internet Service Providers" or "ISPs" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, webhosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by

which to access the Internet including telephone-based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a username or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system and can access the Internet by using his or her account name and password.

g) An "Internet Protocol" or "IP" address is a unique address used by computers or cellular telephones on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer connected to the Internet must have an assigned IP address so that Internet traffic sent from and directed to that computer may be properly directed from its source to its destination. Most ISPs control a particular range of IP addresses. When a customer connects to the Internet using an ISP service, the ISP assigns the computer an IP address. All computers using the same ISP account during that session will share an IP address. The customer's computer retains the IP address for the duration of the Internet session until the user disconnects. The IP address cannot be assigned to a user with a different ISP account during that session. When an Internet user visits any website, that website receives a request for information from that customer's assigned IP address and sends the data to that IP address, thus giving the Internet user access to the website.

h) "Domain Name" refers to the common, easy to remember names associated with an Internet Protocol address. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top-level domains are typically.com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

i) "Log Files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

j) "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

k) "Website" consists of textual pages of information and associated graphic

images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

l) "Uniform Resource Locator" or "Universal Resource Locator" or "URL" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

m) The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

n) The term "computer" includes all types of electronic, magnetic, optical,

electrochemical, or other high speed data processing devices performing logical, arithmetic or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers and network hardware.

o) The terms "storage device" or "storage medium" include any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, SD, and SIM cards, and other magnetic or optical media.

BACKGROUND INFORMATION CONCERNING CHILD PORNOGRAPHY

8. Based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers affect the methods used by people who possess, receive, distribute, and transport child pornography in these ways:

a) Those who create child pornography can produce both still and moving images directly from a common video or digital camera, and other devices that create video and still images, including most cellular telephones and PDAs (e.g., a Blackberry). Images from such devices can be transferred to a computer by attaching the device to the computer using a cable, or by uploading images from the device's memory card directly onto the computer. Once on the computer, images can then be stored, manipulated, transferred, or printed. This includes transfer to some of the same types of devices that are commonly used to create child pornography, such as cellular telephones and PDAs, as well as computers. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. Cellular telephones are routinely backed-up to computers as not to lose any data that is stored on a cellular telephone if that cellular telephone is lost or damaged.

b) The Internet allows any computer to connect to another computer. Electronic contact can be made to literally millions of computers around the world. The Internet allows users, while still maintaining anonymity, to locate (i) other individuals with similar interests in child pornography; and (ii) websites that offer images of child pornography. Child-pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. They can also distribute and collect child-pornography materials with peer-to-peer ("P2P") file sharing, which uses software to link computers together through the Internet to form a network that allows for the sharing of digital files among users on the network. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child-pornography collectors over the Internet.

c) The computer's capability to store images in digital form makes it a common repository for child pornography. Internal and external computer hard drives typically store vast amounts of data, and hard drives with the capacity of 500 or more gigabytes – which can store tens of thousands of images at very high resolution – are not uncommon. Other electronic storage media, such as thumb drives and memory sticks, can store hundreds of images and dozens of videos. Likewise, optical storage media, which includes CD-ROMs and DVDs, and electromagnetic storage media, such as floppy disks, also can hold hundreds of images and multiple videos. Such electronic, optical, and electromagnetic storage media are

very commonly used by those who collect child pornography to store images and videos depicting children engaged in sexually explicit activity. Agents who execute child-pornography search warrants often find electronic, optical, and/or electromagnetic storage media containing child pornography in the same location as or near the computer that was used to obtain, access, and/or store child pornography.

9. My training and experience, and the training and experience of other agents whom I have consulted, have shown the following:

a) Individuals who possess, transport, receive, and/or distribute child pornography often collect sexually explicit materials, which may consist of photographs; magazines; motion pictures; video tapes; books; slides; computer graphics or other images; as well as literature describing sexually explicit activity involving children. Such individuals frequently store their child pornography on multiple electronic, optical, and/or electromagnetic storage media, including not only their computer, but also on external hard drives; floppy disks; CD-ROMs; DVDs; memory sticks; thumb drives; cell phones; PDAs; and other such media. Many of these individuals also collect child erotica, which consists of items that may not rise to the level of child pornography, but which nonetheless serves a sexual purpose involving children.

b) Individuals who possess, transport, receive, and/or distribute child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P; e-mail; e-mail groups; bulletin boards; Internet Relay Chat; newsgroups; instant messaging; and other similar interfaces.

c) Individuals who possess, transport, receive, and/or distribute child pornography often collect; read; copy; or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange, or commercial profit. These names may be maintained in the original medium from which they were derived, in address books or notebooks, on computer storage devices, or merely on scraps of paper.

d) Most individuals who possess, transport, receive, and/or rarely dispose of their sexually explicit materials and commonly retain their collection of child pornography for long periods of time, even for years, in order to retain and gain easy access to child pornography that they have collected, sometimes with considerable effort. These individuals may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. These individuals almost always maintain their collections in the privacy and security of their homes or other secure location. These individuals may keep their collections in locked containers including filing cabinets, safes, or lockboxes. These individuals may also maintain their collections in password-protected or encrypted electronic media. They may keep these passwords, and other information concerning their use of the computer, on handwritten or printed notes that they store in personal areas and around the computer.

e) Possessors, traders, and distributors of child pornography sometimes store their illegal images and videos online in remote storage accounts. Therefore, any records, documents, invoices, and materials in any format or medium that concern online storage or other remote computer storage

could indicate that a person at the TARGET RESIDENCE is storing illegal material in an online storage account.

f) Files, logs, and records relating to P2P files can contain the names of files sent through the P2P service, as well as the date and time the files were transferred. These records could help identify the individual who transferred the child pornography images.

BACKGROUND REGARDING SEIZURE OF COMPUTERS

10. Based upon my knowledge, training, and experience, and the experience of other law enforcement personnel, I know that searches and seizures of evidence from computers commonly require agents to seize most of the computer items (hardware, software, and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. That is almost always true because of the following:

11. Computer storage devices (like hard drives, diskettes, laser disks, and others) store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she may store it in random order with deceptive file names. This requires searching authorities to examine all of the stored data to determine whether it is included in the warrant. This examination process can take weeks or months, depending on the volume of the data stored, and it would be impractical to attempt this kind of data search on-site.

12. Searching computer systems for criminal evidence is a highly technical process requiring expert skills in a properly controlled environment. The vast array of computer hardware and software available today requires even computer experts to specialize in some systems and applications. It is difficult to know before a search which expert should analyze the system and its data. A search of a computer system is an exacting scientific procedure, which is designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password-protected, and other encrypted files. Because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a "booby-trap"), the controlled environment of a laboratory is essential to its

complete and accurate analysis.

13. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices, as well as the central processing unit ("CPU"). In cases like this one, where the evidence consists partly of graphic files, the monitor and printer are also essential to show the nature and quality of the graphic images that the system can produce. In addition, the analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's input/output periphery devices (including related documentation, passwords, and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment. Peripheral devices, which allow users to enter and retrieve data from stored devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly retrieve the evidence sought.

BACKGROUND REGARDING THE INTERNET

14. Through my training and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know that the Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. A user accesses the Internet from a computer network or Internet Service Provider ("ISP") that connects to the Internet. The ISP assigns each user an Internet Protocol ("IP") Address. Each IP address is unique. Every computer or device on the internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates

access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing; that is, they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. The ISP logs the date, time, and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP's record retention policies.

15. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

16. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy or compact disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 250 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds

another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

17. With Internet access, a computer user can transport an image file from the Internet or from another user's computer to his own computer, so that the image file is stored in his computer. The process of transporting an image file to one's own computer is called "downloading." The user can then display the image file on his computer screen and can choose to "save" the image on his computer and/or print out a hard copy of the image by using a printer device (such as a laser or inkjet printer).

18. Importantly, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data.

19. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was

downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

COMMON CHARACTERISTICS OF INDIVIDUALS INVOLVED IN CHILD PORNOGRAPHY AND WHO HAVE A SEXUAL INTEREST IN CHILDREN AND IMAGES OF CHILDREN

20. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who create, view, or receive multiple visual depictions of minors engaged in sexually explicit conduct are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a) Such individuals almost always possess and maintain their "hard copies" or "digital copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years. Such individuals often do not dispose of their collection of sexually explicit material. If the material is discarded or lost due to computer malfunction, these individuals often replenish their supply of child pornography very quickly.

b) Likewise, such individuals often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer or electronic mobile device. These collections are often maintained for several years and are kept close by, usually at the

collector's residence, to enable the individual to view the collection, which is valued highly. Based on my training and experience, I am aware that most people keep their electronic mobile devices on their person or in proximity at all times, even when in their residences.

c) Such individuals also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/ collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

d) Such individuals prefer not to be without their child pornography for any prolonged time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

e) Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[1]

FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that electronic devices

[1] See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

22. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how each device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on each device because:

a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited; Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b) Forensic evidence on a device can also indicate who has used or controlled a device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c) A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d) The process of identifying the exact electronically stored information on a

storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e) Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

23. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant. Further, given the wide geographic proximity of the alleged offenses, it may be prudent to conduct the forensic examination outside of the issuing District.

INVESTIGATION AND FACTS ESTABLISHING PROBABLE CAUSE

24. On October 10, 2023, the FBI received information from the Tennessee Bureau of Investigation (TBI) regarding a joint TBI and Carter County Sheriff's Office (CCSO) investigation into multiple adult males who intentionally met and communicated with a minor female (hereinafter "MINOR VICTIM")[2] online to facilitate, manufacture, receive, and/or produce CSAM, and knowingly induced, coerced, and/or enticed the MINOR VICTIM to engage in illegal sexual activity in or around July-August 2023.

[2] The full identity and telephone number of the MINOR VICTIM is known to law enforcement and was not included this document to protect the MINOR VICTIM's privacy as a potential victim of federal child exploitation crimes.

25. In August 2023, the MINOR VICTIM's parents discovered sexually explicit content – including text messages and photos consistent with CSAM – on the MINOR VICTIM's cellular telephone, a purple Apple iPhone11 (hereinafter "VICTIM TELEPHONE"). The MINOR VICTIM's parents confiscated the VICTIM TELEPHONE and turned it over to the CCSO, which was transferred to the TBI's custody for examination. On November 2, 2023, the TBI requested assistance from the FBI and transferred the VICTIM TELEPHONE into FBI custody for further analysis.[3] The VICTIM TELEPHONE was subsequently examined by the FBI between November 7 and November 13, 2023.

26. A review of the VICTIM TELEPHONE extraction results revealed a total of 221 text messages and six multimedia attachments exchanged between the VICTIM TELEPHONE and cellular telephone number 603-377-0909 (hereinafter "TARGET TELEPHONE"), from July 30 to July 31, 2023, which included three original photos sent by the MINOR VICTIM on July 30, 2023, that were consistent with CSAM. Additionally, AT&T service provider records for the TARGET TELEPHONE revealed three total bi-directional telephone calls between the VICTIM TELEPHONE and the TARGET TELEPHONE from July 30 to July 31, 2023.

27. Based on my investigation to date, which included an examination of public, law enforcement, and telephone service provider records, as set forth below, I believe an individual named Bryan Scott Hoy (hereinafter "HOY") was the user of the TARGET TELEPHONE in July 2023. As such, the government is investigating HOY for receiving and/or possessing material depicting the sexual exploitation of a minor, as well as knowingly using any facility or means of interstate commerce within the territorial jurisdiction of the United States to persuade, induce, entice, and/or coerce a minor to engage in illegal sexual activity, including attempts, in July 2023.

28. As set forth below, I have probable cause to believe that HOY was the user of the

[3] On August 4, 2023, the MINOR VICTIM's parent provided written consent to search the MINOR VICTIM's purple Apple iPhone 11.

TARGET TELEPHONE based on the following:

a) Legal process served to AT&T in November 2023, and May 2024, revealed the following data attributed to the TARGET TELEPHONE:

- Billing/User Information: [redacted]Hoy
- Device: APPLE IPHONE 12
- IMEI: 356599148326144
- IMSI: 310280009935494
- Contact Home Phone: 603-429-0330
- Contact Home Email: RMH1265947@AOL.COM
- Address: 6 Whittier Road, Merrimack, NH 03054 (TARGET RESIDENCE)
- Active Date Range: September 21, 2012 – July 8, 2024

b) Apple subscriber records obtained in July 2024 on the TARGET TELEPHONE, IMEI 356599148326144, and IMSI 310280009935494 revealed the following account information:

- Product: IPHONE 12 BLACK 128GB
- Customer Name: Bryan Hoy
- Apple Logon IDs & Email Addresses: hoy.bryan@gmail.com, hoybryan@icloud.com, airvince8334@aol.com
- Associated Phone Numbers: 603-429-0330, 603-377-0906, 603-377-0909 (TARGET TELEPHONE)
- Street Address: 6 Whittier Road, Merrimack, NH 03054 (TARGET RESIDENCE)

c) Records checks conducted in May 2024 in the National Crime Information Center, LexisNexis Accurint, and Reuters CLEAR, revealed HOY had an active NH driver's license (16646485) and vehicle (2009 Dodge Grand Caravan, red in color, bearing NH license plate number 4572435)

registered to 6 Whittier Road, Merrimack, NH 03054 (TARGET RESIDENCE).

- Surveillance conducted in May and July 2024 observed the 2009 Dodge Grand Caravan, red in color, registered to HOY, parked in the driveway of 6 Whittier Road, Merrimack, NH 03054 (TARGET RESIDENCE), as well as a person who resembled HOY sitting by the front porch of the TARGET RESIDENCE on at least one occasion.

d) Snapchat subscriber records obtained via legal process in May 2024 revealed TARGET TELEPHONE was registered to Snapchat user "bryanhoy19" with the accompanying display name of Bryan Hoy.

e) TikTok subscriber records obtained via legal process in May 2024 revealed TARGET TELEPHONE was registered to TikTok user "bryanhoy0" and IP address 73.89.157.85. An open-source check on the referenced IP address resolved to Merrimack or Concord, New Hampshire.

f) Historical records in Experian indicated, as of June 2013, HOY was associated with the TARGET TELEPHONE and 6 Whittier Road, Merrimack, NH 03054.

g) A Bedford Police Department report, in July 2009, listed the TARGET TELEPHONE NUMBER as associated with HOY.

29. During the examination of the VICTIM TELEPHONE, I located the following derogatory text messages between HOY and the MINOR VICTIM that took place on July 30, 2023, and involved the solicitation, production, manufacture, and receipt of three original photos consistent with CSAM:

a) HOY asked for the MINOR VICTIM's age, to which the MINOR VICTIM responded with a true name and age [fourteen years old].

b) Furthermore, the MINOR VICTIM stated, "I'm younger…I'm sorry.." HOY immediately responded by saying "show me that fucking ass" in addition to the following:

HOY:	It's simple
MINOR VICTIM:	Do you wanna see my ass or not?
HOY:	Show me
MINOR VICTIM:	Naked?
HOY:	Grab that ass
MINOR VICTIM:	[SENT PHOTO CONSISTENT WITH CSAM][4]
HOY:	Grab that shit
MINOR VICTIM:	Nuh uh
MINOR VICTIM:	That's your job
HOY:	I wanna see you lift it
MINOR VICTIM:	No that's a pic I took a few days ago
HOY:	I said rn

c) HOY continued to coerce and verbally abuse the MINOR VICTIM into sending sexually explicit images, two additional times, despite the MINOR VICTIM declining his requests throughout the conversation:

HOY:	You need to understand your place
HOY:	Idc, rn. Grab it
MINOR VICTIM:	Dadddyyyyyy
MINOR VICTIM:	I don't wannaaa
HOY:	Idc, do it
MINOR VICTIM:	Make me.
HOY:	What's the only thing you're good for?
MINOR VICTIM:	That's mean,daddy…
HOY:	Answer…
MINOR VICTIM:	To be daddy's little slut?
HOY:	Say it like you fucking mean it
MINOR VICTIM:	To be daddy's little slut..
HOY:	Name and what you are
MINOR VICTIM:	[true name] and daddy slut
HOY:	Grab that fucking ass rn
HOY:	Now
HOY:	Don't keep daddy waiting
MINOR VICTIM:	But daddyyy
HOY:	But what?

[4] The MINOR VICTIM sent an original photo of herself consistent with CSAM. The photo can be described as the backside and bottom-half of a pubescent Caucasian female torso or midriff partially covered with a black shirt, fully nude buttocks, and the backside upper thighs. File name: IMG_2989.jpg.

MINOR VICTIM:	I don't wannaaa
HOY:	What's your only purpose?
HOY:	Stfu and grab that ass then I know you're for real
MINOR VICTIM:	Ugh
MINOR VICTIM:	Noooo
MINOR VICTIM:	[SENT PHOTO CONSISTENT WITH CSAM][5]
HOY:	I said fucking grab it
MINOR VICTIM:	You said night
MINOR VICTIM:	Not until you call me
HOY:	What's the only thing you're good for?
HOY:	Well?
HOY:	?
HOY:	Don't keep daddy waiting
HOY:	?
MINOR VICTIM:	My mom called me give a second
HOY:	Show me again
MINOR VICTIM:	Show you what?
HOY:	That body
MINOR VICTIM:	[SENT PHOTO CONSISTENT WITH CSAM][6]

CONCLUSION

30. Based on the aforementioned information, I have probable cause to believe that violations of Title 18 U.S.C. § 2252(a)(2), Title 18 U.S.C. § 2252A(a)(5)(A)(B) & (b)(2), and Title 18 U.S.C. § 2422(b) have been committed by HOY, and that the items described in Attachment B, which are evidence, fruits, contraband, and instrumentalities of those violations, will be found at the TARGET ADDRESS and on the person of HOY.

31. By this affidavit, I request that the Court issue a warrant authorizing a search of

[5] The MINOR VICTIM sent an original photo of herself consistent with CSAM. The photo can be described the fully nude buttocks, vagina/labia, and backside upper thighs of a blonde-haired pubescent Caucasian female kneeling away from the camera, while on top of a cushioned dark brown chair and in a room with yellow walls, a window with curtains drawn, and a white ceiling. The right mid-to-upper thigh of the pubescent Caucasian female appeared to have at least one bruise or scar visible in the photo. File name: IMG_2842.jpg.

[6] The MINOR VICTIM sent an original photo of herself consistent with CSAM. The photo can be described as a fully nude blonde-haired pubescent Caucasian female, likely between the age of 12 to 16, kneeling toward the camera and next to – or on top of – a cushioned chair/couch with her breasts, midriff, and upper thighs fully exposed. The pubescent Caucasian female in the photo appeared to have a pink scrunchie on her left and right wrist, two hair ties on her left wrist, and at least three additional bracelets on her left and right wrist. The background of the photo appeared to show a drawn black and white checkered curtain, with sunlight shining thru, against a white or light-yellow wall. File name: IMG_2832.jpg.

the TARGET ADDRESS as described in Attachment A1 and HOY as described in Attachment A2, as well as the search and seizure of the items listed in Attachment B.

REQUEST FOR SEALING

32. Your affiant respectfully requests the Court order the entirety of all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents contain sensitive information and discuss an ongoing criminal investigation, that is neither public nor known to all of the targets of the investigation, and not all of the targets of this investigation have been arrested or indicted. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

33. The above information is true and correct to the best of my knowledge, information, and belief.

Respectfully submitted,

/s/ Andrew P. LaRose
Andrew P. LaRose
Special Agent
Federal Bureau of Investigation

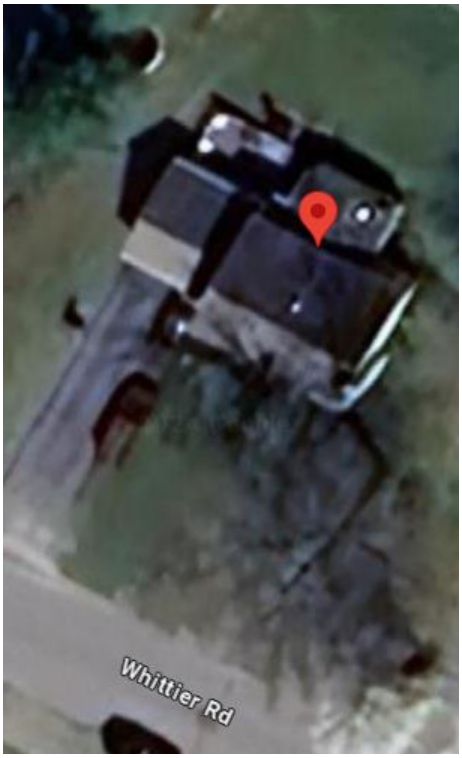
Sworn and subscribed to telephonically
This 7th Day of August, 2024.

/s/ Andrea K Johnstone
Andrea K. Johnstone
United States Magistrate Judge

ATTACHMENT A – TARGET RESIDENCE

PROPERTY TO BE SEARCHED BY THE GOVERNMENT

The residence at 6 Whittier Road, Merrimack, New Hampshire 03054 is a 2,342 square-foot multi-level, single-family, colonial style home with four bedrooms, three bathrooms, a partially finished basement, and attached parking garage, sitting on 0.44 acres of land facing Whittier Road and surrounded by tall trees on the right, left and back side of the house. The exterior has yellow or beige colored vinyl siding, as well as brown asphalt shingled roofing. The driveway is paved in black asphalt and located on the front left-side of the house, leading to a two-car garage facing Whittier Road. A chimney is located on the right side of the house. The front of the house has four windows on the first level, and five windows on the second level facing Whittier Road, all of which are bordered with raised navy or dark green shutters. The front entry door of the residence is painted navy, or dark green, with an overhang and is located on the first level directly beneath the third second-level window. There are about three steps leading up to the small porch and entry door, as well as a wooden bench in front of two first level windows on the right-side facing Whittier Road. The back side of the home contains a possible porch on the left side, with a pool in the backyard about 50-100 feet from the house.



ATTACHMENT A – HOY

PERSON TO BE SEARCHED BY THE GOVERNMENT

BRYAN SCOTT HOY, date of birth [redacted]1988, NH driver's license number 16646485, 6 Whittier Road, Merrimack, NH 03054, and any personal items in his possession, for the property and personal belongings (including computers and computer media and cellular telephones) described in Attachment B.

ATTACHMENT B

Particular Items to be Searched & Seized by the Government

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of a crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18 U.S.C. § 2252(a)(2) – distribution or receipt of child pornography, Title 18 U.S.C. § 2252A(a)(5)(A)(B) & (b)(2) – possession or knowingly accessing with intent to view child pornography (including attempts or conspiracies), and Title 18 U.S.C. § 2422(b) – inducement, coercion and/or enticement of a minor, including:

1. Any and all computer(s), computer hardware, computer software (including programs to run operating systems and applications such as word and image processing, communications programs, instant messaging, and peer-to-peer software), storage media, computer-related documentation, computer passwords and data-security devices, videotapes, video-recording devices, video-recording players, and video display monitors that are located in HOY's living space or may be used by HOY to: visually depict child pornography; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, or information pertaining to an interest in child pornography.

2. Any and all electronic devices, including computer equipment and mobile devices used by HOY that can connect to the Internet and record pictures and video.

3. Any and all routers, modems, and network equipment used by HOY to connect computers to the Internet.

4. In electronic or digital format, all originals, computer files, records, copies, and negatives of child pornography or visual depictions of minors engaged in sexually explicit conduct, as such terms defined in Title 18 U.S.C § 2256.

5. Any and all notes, documents, information, records, or correspondence, in electronic or digital format (including, but not limited to, letters, diaries, word processing documents, address books, email messages, chat logs and electronic messages, other digital data files, and web cache information):

a) Pertaining to or concerning the possession, receipt, transmission, distribution, or production of child pornography or to the possession, receipt, transmission, distribution, or production of visual depictions of minors engaged in sexually explicit conduct, as such terms are defined in Title 18 U.S.C. § 2256.

b) Relating to an interest in child pornography, whether transmitted or received; pertaining to an interest in child exploitation, child erotica, pedophilia, or sexual abuse of children; relating to the persuading, inducing, enticing, or coercing of minors to engage in prostitution or any sexual activity; or pertaining to the transfer of obscene matter to minors.

c) Identifying any person transmitting, through interstate or foreign commerce, by any means, any child pornography or any visual depictions of minors engaged in sexually explicit conduct, as such terms are defined in Title 18 U.S.C. § 2256.

d) Containing names or lists of names and addresses of individuals who have

been contacted via use of the computer(s) or by other means for the purpose of distributing, receiving, or producing child pornography or visual depictions of minors engaged in sexually explicit conduct, as such terms are defined in Title 18 U.S.C. § 2256.

e) Reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as such terms are defined in Title 18 U.S.C. § 2256.

f) Concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

g) Concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

h) Concerning any accounts with an Internet Service Provider.

i) Concerning online storage, cloud storage, or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show a connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

j) Pertaining to the preparation, purchase, and acquisition of names or lists of names (for example, address books, mailing lists, supplier lists) to be used in connection with the purchase, sale, trade, or transmission through interstate or foreign commerce by any means any child pornography or any visual depiction of minors engaged in sexually explicit conduct, as such terms are defined in Title 18 U.S.C. § 2256.

6. Any and all materials or items owned, possessed, used, or accessed by HOY that are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex educations, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings. "Child erotica" may also include, in this context, sex aids and/or toys.

7. Records or other items which evidence ownership or use of cellular telephones, computer equipment found in HOY's living space within the residence described above, or on the person of HOY, including, but not limited to sales receipts, bills for Internet access, and handwritten notes.

8. For any cellular telephone, computer, or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, the "Seized Item"):

a) Evidence of who used, owned, or controlled the Seized Item at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and

passwords, documents, browsing history, user profiles, email, email contacts, chats, instant messaging logs, photographs, and correspondence.

b) Evidence of software that would allow others to control the Seized Item, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

c) Evidence of the lack of such malicious software.

d) Evidence indicating how and when the Seized Item was accessed or used to determine the chronological context of access, use, and events relating to crime under investigation and to the user.

e) Evidence of the attachment to the Seized Item of other storage devices or similar containers for electronic evidence.

f) Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Seized Item.

g) Evidence of the times the Seized Item was used by HOY.

h) Passwords – including biometric passwords (i.e., fingerprints and/or facial recognition access), encryption keys, and other access devices that may be necessary to access the Seized Item.

i) Documentation and manuals that may be necessary to access the Seized Item or to conduct a forensic examination of the Seized Item.

j) Records of, or information about, Internet Protocol addresses used by the Seized Item.

k) Records or information about the Seized Item's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorited" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

l) Contextual information necessary to understand the evidence described in this attachment.

9. This warrant authorizes a review of electronically stored information, communications, other records, and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

10. During the execution of the search of the entities described in Attachment A, law enforcement personnel are also specifically authorized to compel HOY to display any biometric features, including pressing his fingers, including thumbs, against and/or putting his face before the sensor, or any other security feature requiring biometric recognition, of any of the devices found in HOY's living space within the residence which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments, for the purpose of attempting to unlock the device's security features in order to search the contents as authorized by this warrant.

11. This warrant does not authorize law enforcement personnel to compel any other

individuals found at the residence to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any device. Further, this warrant does not authorize law enforcement personnel to request that HOY state or otherwise provide the password or any other means that may be used to unlock or access the devices, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the device.

12. *Definitions*, as used throughout this attachment:

a) The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions. Examples include desktop computers, notebook computers, cellular mobile phones, tablets, server computers, and network hardware.

b) The term "storage medium" or "storage media" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.